(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000347942 A

(43) Date of publication of application: 15.12.00

(51) Int. Cl G06F 12/14
G06F 11/22
G06F 15/78

(21) Application number: 11158256

(22) Date of filing: 04.06.99

(71) Applicant: TOSHIBA CORP

(72) Inventor: TANABE TETSUYA
ASAI EIICHI

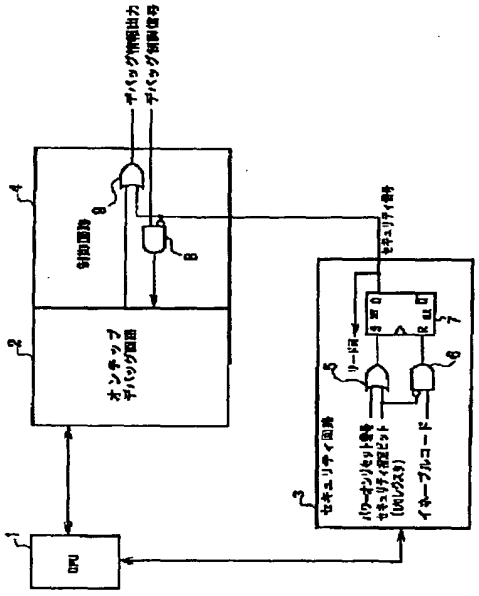
(54) INFORMATION PROCESSOR

(57) Abstract:

PROBLEM TO BE SOLVED: To protect information stored in a ROM from an illegal access caused by a debug tool provided externally.

SOLUTION: An on-chip debug circuit 2 mounted in the information processor is made invalid by power-on reset, and an on-chip debug ICE(in-circuit emulator) is prohibited from accessing an incorporated ROM. The invalidation of the circuit 2 is released by setting an I/O register released to a user by a user program.





(1)

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－347942
（Ｐ２０００－３４７９４２Ａ）
(43)公開日　平成12年12月15日(2000.12.15)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| G06F 12/14 | 310 | G06F 12/14 | 310 | E 5B017 |
| 11/22 | 340 | 11/22 | 340 | A 5B048 |
| 15/78 | 510 | 15/78 | 510 | C 5B062 |

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平11－158256

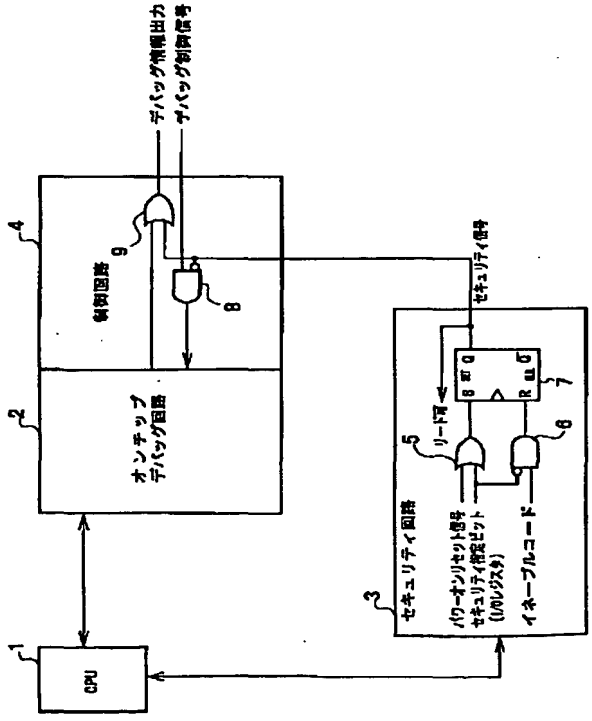
(22)出願日　平成11年６月４日(1999.6.4)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　田部　徹也
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内
(72)発明者　浅井　栄一
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝マイクロエレクトロニクスセンター内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】情報処理装置

(57)【要約】
【課題】　この発明は、ＲＯＭに記憶された情報を、外部に設けられたデバッグツールによる不正アクセスから保護することを課題とする。
【解決手段】　この発明は、情報処理装置内に実装されているオンチップデバッグ回路２をパワーオンリセットにより無効化し、オンチップデバッグＩＣＥによる内蔵ＲＯＭのアクセスを禁止し、オンチップデバッグ回路の無効化は、ユーザプログラムによりユーザに開放されたＩ／Ｏレジスタの設定により解除されるように構成される。



メモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力制御を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化してセキュリティを設定し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、セキュリティ指定ビットと、このセキュリティ指定ビットのリセットをイネーブルとするイネーブルコードとを受けて、前記オンチップデバッグ回路の機能を有効化してセキュリティを解除し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする。

【０００７】第２の手段は、前記第１の手段において、前記セキュリティー指定ビットは、電源投入時にセットされて前記オンチップデバッグ回路の機能が無効化されセキュリティが設定されている状態、又は前記ＲＯＭに記憶されたセキュリティ解除プログラムによりリセットされて前記オンチップデバッグ回路の機能が有効化されセキュリティが解除されている状態を有することを特徴とする。

【０００８】第３の手段は、前記第１の手段において、前記セキュリティ回路は、前記オンチップデバッグ回路を無効化する際に、一部機能を有効化してなることを特徴とする。

【０００９】第４の手段は、外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、予め登録されたコードと外部から与えられたパスワードとを照合して両者が一致した場合には、前記オンチップデバッグ回路の機能を有効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする。

【００１０】第５の手段は、外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、前記エミュレータから暗号化されて前記情報処理装置に与えられるデバッグに必要な信号を復号化し、前記情報処理装置のデバッグ結果を暗号化して前記エミュレータに出力する暗号化回路とを有することを特徴とする。

【００１１】

【発明の実施の形態】以下、図面を用いて本発明の実施形態を説明する。

【００１２】図１はこの発明の一実施形態に係る情報処理装置の要部構成を示す図であり、図２はデバッグの手順を示すフローチャートである。

【００１３】図１において、この実施形態の情報処理装置のマイコンは、ＣＰＵ１、図示しないＲＯＭや周辺回路に加えて、前述したと同様のオンチップデバッグ回路２、セキュリティ回路３、制御回路４を備えて構成されている。

【００１４】セキュリティ回路３は、電源投入時にマイコンをリセットするパワーオンリセット信号とセキュリティ指定ビットを入力とする論理和（ＯＲ）ゲート５と、セキュリティ指定ビットの反転とセキュリティ指定ビットのリセットをイネーブルとするイネーブルコードを入力とする論理積（ＡＮＤ）ゲート６と、ＯＲゲート５の出力をセット（Ｓ）入力としＡＮＤゲート６の出力をリセット（Ｒ）入力とし出力（Ｑ）をセキュリティ信号として制御回路４に与えるレジスタ（ＲＳフリップフロップ）７を備え、パワーオンリセット信号を受けてオンチップデバッグ回路２の機能を無効化してセキュリティを設定し、エミュレータによるメモリの記憶情報の読み出し、特にオンチップデバッグＩＣＥ（インサーキットエミュレータ）によるＲＯＭの記憶情報の読み出しを禁止し、リセットされたセキュリティ指定ビットかつイネーブルコードを受けて、オンチップデバッグ回路２の機能を有効化してセキュリティを解除し、オンチップデバッグＩＣＥによるＲＯＭの記憶情報の読み出しを可能にする。

【００１５】制御回路４は、セキュリティ回路３から与えられるセキュリティ信号の反転と、オンチップデバッグＩＣＥから与えられてマイコンをデバッグするのに必要となる信号のデバッグ制御信号を入力するＡＮＤゲート８と、セキュリティ信号とオンチップデバッグ回路２から与えられるデバッグ結果を入力としデバッグ情報出力をオンチップデバッグＩＣＥに出力するＯＲゲート９を備え、セキュリティ信号がセキュリティ回路３から与えられてセキュリティが設定されている場合には、デバッグ制御信号の入力ならびにデバッグ情報の出力を禁止する。

【００１６】次に、この実施形態では、以下のような方式でマイコン内のオンチップデバッグ回路２の動作を制御する。

【００１７】セキュリティ用のセキュリティ指定ビットをＩ／Ｏレジスタに設ける。このセキュリティ指定ビットは、パワーオン時に“１”（セキュリティ有効）にセットされ、オンチップデバッグ回路２は、パワーオンリセットによってオンチップデバッグ回路２の機能が無効となるように初期化される。外部に接続されるオンチッ

7

オンリセットを利用することにより、一度セキュリティが解除された後は、マイコンの電源を落とすまで、制限無くオンチップデバッグＩＣＥを使用できる。

【００２８】次に、この発明の他の実施形態について説明する。

【００２９】この実施形態の特徴とするところは、上記実施形態のセキュリティ解除判定ルーチンにおいて、予めマイコン内に設定したコードと、外部入力やオンチップデバッグＩＣＥからの入力を比較して判定するパスワード方式としてセキュリティの解除プログラムを作成せず、図１に示すセキュリティ回路３に代えて、パワーオンリセット信号によりオンチップデバッグ回路２の機能を無効化し、オンチップデバッグＩＣＥによるＲＯＭの記憶情報の読み出しを禁止し、予め登録されたコードと外部から与えられたパスワードを照合して両者が一致した場合には、オンチップデバッグ回路２の機能を有効化し、オンチップデバッグＩＣＥによるＲＯＭの記憶情報の読み出しを可能にする、パスワード判定回路を含むセキュリティ解除回路を組み込む構成を採用したことにある。このような実施形態にあっても、上記実施形態と同様な効果を得ることができる。

【００３０】次に、この発明の他の実施形態について説明する。

【００３１】この実施形態の特徴とするところは、前述した図１に示す実施形態でのセキュリティ有効時に、オンチップデバッグ機能のすべてを禁止するのではなく、一部のデバッグ機能を許可する、例えばユーザアプリケーションにおいて使用するデバッグ機能があれば、その部分のみ常時許可するようにしたことにある。

【００３２】一方、オンチップデバッグＩＣＥから暗号化されて情報処理装置に与えられるデバッグに必要な信号を復号化し、情報処理装置のデバッグ結果を暗号化してオンチップデバッグＩＣＥに出力する暗号化回路を設け、セキュリティ有効時に、デバッグ情報を暗号化してオンチップデバッグＩＣＥへ出力し、オンチップデバッグＩＣＥ側でその暗号の解読を制御し、正規ユーザーのみ暗号を解読してデバッグできるようにしてもよい。このような実施形態にあっても、上記実施形態と同様な効果を得ることができる。

8

【００３３】

【発明の効果】以上説明したように、この発明によれば、パワーオンリセットにより情報処理装置内に実装されているオンチップデバッグ回路を無効化しセキュリティを設定し、オンチップデバッグＩＣＥによる内蔵ＲＯＭのアクセスを禁止し、ユーザプログラムにより設定制御されるセキュリティ指定ビットに基づいてセキュリティが解除されるようにしたので、ＲＯＭに記憶された情報を、外部に設けられたデバッグツールによる不正アクセスから保護することが可能となる。また、セキュリティの解除方法は、ユーザが自由に設定できるため、セキュリティの解除方法が無限となり、守秘性が高くなる。さらに、セキュリティの制御にパワーオンリセットを利用することにより、一度セキュリティが解除された後は、電源がオフされるまでオンチップデバッグＩＣＥを制限なく使用することができる。

【図面の簡単な説明】

【図１】この発明の一実施形態に係る情報処理装置の要部構成を示す図である。

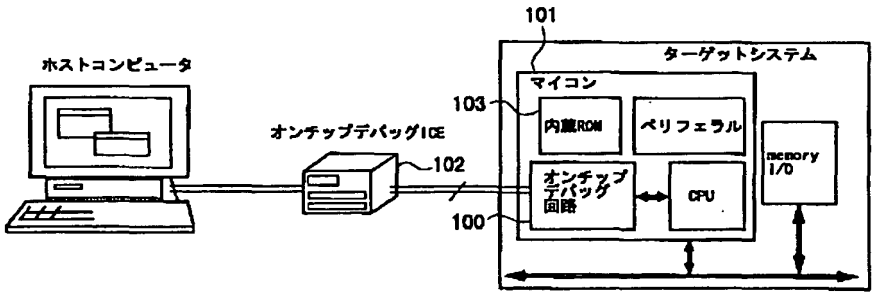
【図２】図１に示す実施形態の動作手順を示すフローチャートである。

【図３】ターゲットシステムをデバッグする従来のシステムを示す図である。

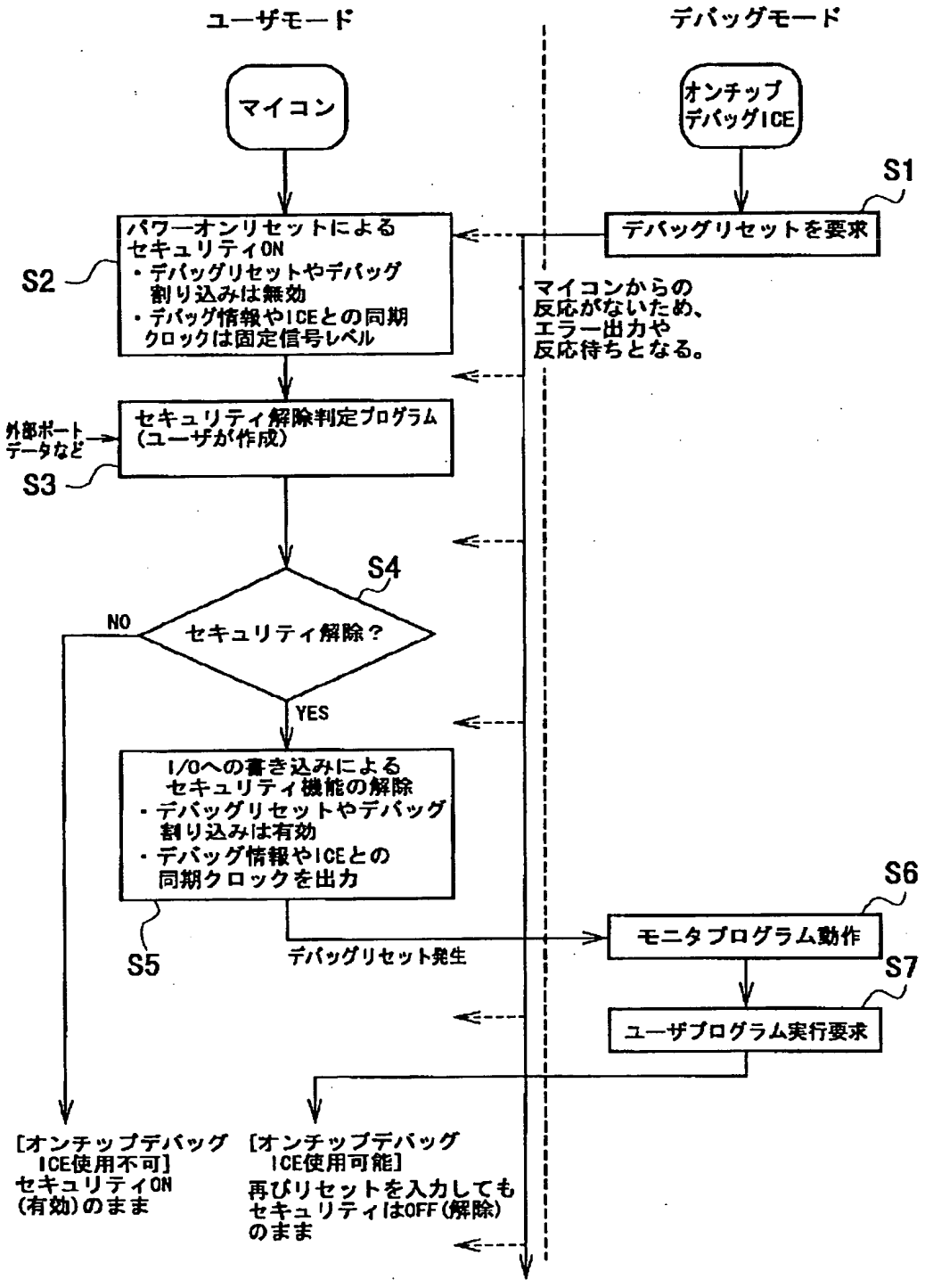
【符号の説明】

１　ＣＰＵ
２　オンチップデバッグ回路
３　セキュリティ回路
４　制御回路
５，６，８，９　論理ゲート
７　レジスタ

【図３】



【図２】


ユーザモード
デバッグモード
マイコン
オンチップ
デバッグICE
S1
デバッグリセットを要求
パワーオンリセットによる
セキュリティON
・デバッグリセットやデバッグ
割り込みは無効
・デバッグ情報やICEとの同期
クロックは固定信号レベル
S2
マイコンからの
反応がないため、
エラー出力や
反応待ちとなる。
外部ポート
データなど
セキュリティ解除判定プログラム
(ユーザが作成)
S3
S4
セキュリティ解除？
NO
YES
I/Oへの書き込みによる
セキュリティ機能の解除
・デバッグリセットやデバッグ
割り込みは有効
・デバッグ情報やICEとの
同期クロックを出力
S5
デバッグリセット発生
S6
モニタプログラム動作
S7
ユーザプログラム実行要求
[オンチップデバッグ
ICE使用不可]
セキュリティON
(有効)のまま
[オンチップデバッグ
ICE使用可能]
再びリセットを入力しても
セキュリティはOFF(解除)
のまま